Memoria sobre las condiciones para la solubilidad de ecuaciones por radicales

Por

Évariste Galois

Traducción de

Emilio Méndez Pinto

Edición digital para la Biblioteca Digital del ILCE
Título original: *Memoir on the Conditions for the Solvability of Equations by Radicals*

La memoria ofrecida aquí está tomada de un trabajo que tuve el privilegio de presentar ante la *Academia* hace un año. Ya que este trabajo no ha sido incluido, y ya que las proposiciones que sostenía son otra vez dudosas, me contento con ofrecer los principios generales de la teoría en una forma sintética, y con ofrecer *sólo una* aplicación de mi teoría. Ruego a mis jueces que por lo menos lean estas pocas páginas con cuidado.

Aquí encontraremos una *condición* general que es *satisfecha* por *toda ecuación soluble por radicales*, y que, a la inversa, asegura su solubilidad. Aplicaremos esta condición sólo a ecuaciones cuyo grado es un número primo. Aquí está el teorema ofrecido por nuestro análisis:

Para que una ecuación de grado primo que no tenga divisores conmensurables sea soluble por radicales, es necesario y suficiente que todas las raíces sean funciones racionales de cualesquiera dos de las raíces.

Las demás aplicaciones de la teoría son, por sí mismas, teorías particulares por derecho propio. Más aún, requieren de la teoría de números y de un algoritmo particular, así que las guardaremos para otra ocasión. En parte, tienen una relación con las ecuaciones modulares de la teoría de funciones elípticas que, como demostraremos, no pueden ser resueltas por radicales.

Enero 16, 1831

E. GALOIS

PRINCIPIOS

Comenzaré estableciendo algunas definiciones y una serie de lemas ya bien conocidos.

Definiciones. Se dice que una ecuación es reducible cuando admite divisores racionales; irreducible en el caso contrario.

Es necesario explicar qué queremos decir con la palabra *racional*, ya que será utilizada a menudo.

Cuando *todos* los coeficientes de una ecuación son tanto numéricos como racionales, cuando decimos que esta ecuación puede ser dividida racionalmente simplemente queremos decir que la ecuación puede ser partida en factores que tienen coeficientes numéricos y racionales.

Pero cuando no *todos* los coeficientes de una ecuación son numéricos y racionales, entonces cuando decimos que esta ecuación puede ser dividida racionalmente por un divisor racional debemos referirnos a un divisor cuyos coeficientes están expresados en una función racional con coeficientes de la ecuación dada; y en general, por una cantidad racional nos referimos a una cantidad que es expresada como una función racional de los coeficientes de la ecuación dada.

Hay más: sería conveniente considerar como racional toda función racional de un cierto número de cantidades determinadas, suponiendo que estas cantidades están dadas de antemano. Por ejemplo, podríamos elegir una cierta raíz de un número entero y considerar como racional cada función racional de este radical.

Cuando llegamos a considerar ciertas cantidades conocidas de esta manera, diremos que las *añadimos* a una ecuación que queremos resolver. Diremos que estas cantidades son *añadidas* a la ecuación.

Habiendo establecido esto, llamaremos *racional* a toda cantidad que es expresada en una función racional de los coeficientes de la ecuación dada y de un cierto número de cantidades que ya han sido *añadidas* a la ecuación y que han sido acordadas arbitrariamente.

Cuando recurramos a la ayuda de ecuaciones auxiliares, éstas serán racionales si sus coeficientes son racionales en nuestro sentido.

Además de esto, podemos ver que las propiedades y las dificultades de una ecuación pueden ser completamente distintas dependiendo de las cantidades añadidas a ella. Por ejemplo, la añadidura de una cantidad puede hacer que una ecuación irreducible sea reducible.

Así, cuando añadimos una raíz de una de las ecuaciones auxiliares de Gauss a la ecuación $\frac{x^n - 1}{x - 1} = 0$, donde n es un número primo, esta ecuación se descompone en factores y, consecuentemente, se vuelve reducible.

Las sustituciones son la transición de una permutación a otra.

La permutación de la que partimos para indicar las sustituciones es completamente arbitraria cuando se trata de funciones, porque no hay razón alguna por la cual, en una función de muchas letras, una letra deba ocupar una posición en lugar de otra.

Sin embargo, ya que difícilmente podemos formarnos la idea de una sustitución sin formarnos [la idea] de una permutación, con frecuencia hablaremos de

permutaciones, y consideraremos las sustituciones únicamente como el paso de una permutación a otra.

Cuando lleguemos a agrupar las sustituciones, haremos que todas vengan de la misma permutación.

Ya que esto siempre se reduce a cuestiones sobre si el arreglo original de las letras no influye nada en absoluto, en los grupos que consideraremos habremos de tener las mismas sustituciones sea cual sea la permutación de la que partimos. Por lo tanto, si en un grupo de este tipo tenemos las sustituciones *S* y *T*, podemos estar seguros de tener la sustitución *ST*.

Estas son las definiciones que pensamos deben ser recordadas.

Lema I. Una ecuación irreducible no puede tener una raíz en común con una ecuación racional sin dividirla.

Porque el máximo común divisor de la ecuación irreducible y la otra ecuación racional seguirían siendo racionales, por lo tanto, etcétera.

Lema II. Dada cualquier ecuación cuyas raíces son $a, b, c, \ldots$, donde ningunas de las raíces son iguales entre sí, siempre podemos formar una función *V* de estas raíces tal que ninguno de los valores que obtenemos al permutar las raíces en esta función sean iguales de ninguna manera.

Por ejemplo, uno puede establecer que

$$V = Aa + Bb + Cc + \ldots,$$

A, *B*, *C* siendo números enteros apropiadamente elegidos.

Lema III. Una vez elegida la función *V* tal como fue indicado en el lema anterior, ésta tendrá la propiedad de que cada una de las raíces de la ecuación dada puede ser expresada racionalmente en una función de *V*.

En efecto, sea

$$V = \varphi(a, b, c, d, \ldots), \text{ o}$$

$$V - \varphi(a, b, c, d, \ldots) = 0.$$

Multipliquemos entre sí todas las ecuaciones de este tipo que obtenemos al permutar todas las letras, sólo permaneciendo fija la primera letra; entonces tendremos la siguiente expresión:

$$[V - \varphi(a, b, c, d, \ldots)][V - \varphi(a, b, c, d, \ldots)][V - \varphi(a, b, c, d, \ldots)] \ldots,$$

que es simétrica en *b*, *c*, *d*, …, y que, consecuentemente, puede ser escrita como una función de *a*. Así, tendremos una ecuación de la forma

$F(V, a) = 0$.

Pero yo digo que podemos extraer el valor de *a* de esta expresión. Para esto es suficiente con encontrar la solución común de esta ecuación y de la ecuación dada. Esta solución es la única solución común a las dos ecuaciones, porque no podemos tener, por ejemplo, que

$F(V, b) = 0$,

en donde esta ecuación tiene un factor común con la otra ecuación de este tipo, a menos que una de las funciones $\varphi(a,...)$ fuese igual a una de las funciones $\varphi(b,...)$, pero esto es contrario a nuestra hipótesis.

De esto se sigue que *a* es expresada en una función racional de *V*, y que es lo mismo para todas las demás raíces.

Esta proposición[1] la menciona Abel, sin demostración alguna, en su memoria póstuma sobre las funciones elípticas.

Lema IV. Supongamos que hemos formado la ecuación en V, y que hemos tomado uno de sus factores irreducibles de tal manera que V es una raíz de una ecuación irreducible. Sean $V, V', V'', \dots$ *las raíces de esta ecuación irreducible. Si* $a = f(V')$ *es una de las raíces de la ecuación dada, la propia* $f(V')$ *será una raíz de la ecuación dada*.

En efecto, al multiplicar entre sí todos los factores de la forma $V - \varphi(a, b, c, ...)$, donde hemos realizado toda permutación posible de todas las letras excepto una, tendremos una ecuación racional en *V* que necesariamente será divisible por la ecuación en cuestión; así, V' debe obtenerse al intercambiar las letras en la función *V*. Sea $F(V, a) = 0$ la ecuación que obtenemos al permutar todas las letras en *V* excepto la primera letra. De esta forma tendremos $F(V', b) = 0$, donde *b* podría ser igual a *a*, pero debe ser una de las raíces de la ecuación dada; consecuentemente, así como de la ecuación dada y de $F(V, a) = 0$ resulta que $a = f(V)$, también cuando son combinadas la ecuación dada y $F(V', b) = 0$ se sigue que $b = f(V')$.

[1] Es notable que de esta proposición podamos concluir que toda ecuación depende de alguna ecuación auxiliar tal que todas las raíces de esta nueva ecuación son funciones racionales una de otra; la ecuación auxiliar en *V* está en este caso. Permítanme añadir que esta observación es meramente una curiosidad. En realidad, una ecuación que tenga esta propiedad no es, por lo general, más fácil de resolver que una que no la tenga.

PROPOSICIÓN I

Teorema. Haya una ecuación cuyas m raíces son a, b, c,… Siempre habrá un grupo de permutaciones de las letras a, b, c,… que tiene la siguiente propiedad:

(1) toda función de raíces que es invariante[2] *bajo las sustituciones de este grupo es conocida racionalmente;*

(2) a la inversa, toda función de raíces que es determinable racionalmente, es invariante bajo las sustituciones de este grupo.

(En el caso de las ecuaciones algebraicas, este grupo no es otro que la colección de $1\cdot 2\cdot 3,...,m$ permutaciones posibles de las *m* letras, porque aquí las funciones simétricas por sí solas son determinables racionalmente.)

(En el caso de la ecuación $\frac{x^n-1}{x-1}=0$, si dejamos que $a=r, b=r^g, c=r^{g^2},...$, donde *g* es una raíz primitiva, el grupo de permutaciones simplemente será:

abcd ……… k

bcd ………ka

cd ……… kab

………

kabc ……… j

En este caso particular, el número de permutaciones es igual al grado de la ecuación, y la misma cosa se obtendrá en el caso de una ecuación cuyas todas raíces son funciones racionales una de otra.)

Demostración. Sea cual sea la ecuación dada, podremos encontrar una función racional *V* de sus raíces tal que todas las raíces son funciones racionales de *V*. Dadas estas ecuaciones, consideremos la ecuación irreducible de la cual *V* es una raíz (lemas III y IV). Sean $V, V', V'', ...V^{(n-1)}$ las raíces de esta ecuación.

Sean $\varphi V, \varphi_1 V, \varphi_2 V, ..., \varphi_{m-1} V$ las raíces de la ecuación propuesta. Escribamos las siguientes *n* permutaciones de las raíces:

[2] Aquí llamaremos invariante a una función no sólo cuando la forma es invariante bajo las sustituciones de sus raíces una para la otra, sino también cuando el valor numérico de la función no varía bajo estas sustituciones. Por ejemplo, si $Fx=0$ es una ecuación, Fx es una función de raíces que no varía bajo ninguna sustitución. Cuando decimos que una función es conocida racionalmente, queremos decir que su valor numérico es expresable como una función racional con coeficientes de la ecuación y de las cantidades añadidas.

(V)	φV	$\varphi_1 V$	$\varphi_2 V$	, … ,	$\varphi_{m-1} V$
(V')	$\varphi V'$	$\varphi_1 V'$	$\varphi_2 V'$	, … ,	$\varphi_{m-1} V'$
(V'')	$\varphi V''$	$\varphi_1 V''$	$\varphi_2 V''$	, … ,	$\varphi_{m-1} V''$
……	……	……	……	……	……
$(V^{(n-1)})$	$\varphi V^{(n-1)}$	$\varphi_1 V^{(n-1)}$	$\varphi_2 V^{(n-1)}$	, … ,	$\varphi_{(m-1)} V^{(n-1)}$

Yo digo que este grupo de permutaciones tiene la propiedad mencionada.

(1) Toda función de raíces *F* que es invariante bajo las sustituciones de este grupo puede escribirse así: $F = \psi V$, y entonces tendremos que

$$\psi V = \psi V' = \psi V'' = ... = \psi V^{(n-1)} .$$

De esta manera puede determinarse racionalmente el valor de *F*.

(2) A la inversa, si una función *F* es determinable racionalmente y establecemos que $F = \psi V$, debemos tener que

$$\psi V = \psi V' = \psi V'' = ... = \psi V^{(n-1)} ,$$

porque la ecuación en *V* no tiene un divisor conmensurable y porque *V* satisface la ecuación $F = \psi V$, *F* siendo una cantidad racional. Así, la función *F* será necesariamente invariante bajo las sustituciones del grupo escrito arriba.

Así, este grupo tiene la doble propiedad a la cual se refiere el teorema establecido. De esta manera es demostrado el teorema.

Llamaremos al grupo en cuestión el grupo de la ecuación.

Escolio 1. Es evidente que en el grupo de permutaciones que nos ocupa aquí, el arreglo de las letras no debe considerarse en absoluto, sino sólo [deben considerarse] las sustituciones de las letras bajo las cuales pasamos de una permutación a otra.

Así pues, podemos darnos una primera permutación de manera arbitraria siempre que las demás permutaciones se deriven siempre de las mismas sustituciones de letras. Siendo esto así, el nuevo grupo formado de esta manera obviamente tendrá las mismas propiedades que el primer grupo, porque en el teorema anterior sólo nos ocupamos de las sustituciones que podemos hacer en las funciones.

Escolio 2. Las sustituciones son independientes incluso del número de raíces.

PROPOSICIÓN II

Teorema. Si añadimos la raíz r de una ecuación irreducible auxiliar a una ecuación dada

(1) una de dos cosas pasará: o bien el grupo de la ecuación no cambiará, o bien será partido en p grupos cada uno perteneciendo a la ecuación dada respectivamente cuando añadimos cada una de las raíces de la ecuación auxiliar a ella;

(2) [si sucede lo segundo, entonces] estos grupos tendrán la notable propiedad de que pasaremos de uno a otro al poner a trabajar la misma sustitución de las letras en todas las permutaciones del primer grupo.

(1) Si, después de la añadidura de *r*, la ecuación en *V* (de la que hablamos antes) sigue siendo irreducible, es claro que el grupo de la ecuación no cambiará. Si, por el contrario, la ecuación en *V* es reducida, entonces la ecuación en *V* será partida en *p* factores todos del mismo grado y de la forma

$$f(V,r)\times f(V,r')\times f(V,r'')\times\ldots,$$

r, r', r'', siendo los demás valores de *r*. De esta manera, el grupo de la ecuación dada también será partido en grupos cada uno con el mismo número de permutaciones, ya que una permutación corresponde a cada valor de *V*. Estos grupos serán los de la ecuación dada, respectivamente, cuando a ella añadamos sucesivamente $r, r', r'',\ldots$.

(2) Hemos visto antes que todos los valores de *V* son funciones racionales entre sí. Siguiendo esto, supongamos que mientras que *V* es una raíz de $f(V,r)=0$, $F(V)$ es otra raíz de $f(V,r)=0$; es claro que, del mismo modo, si V' fuese una raíz de $f(V,r')=0$, $F(V')$ será otra raíz de $f(V,r')=0$, porque tendremos que

$$f[F(V'),r] = \textit{una función divisible por } f(V,r).$$

Así, (lema IV)

$$f[F(V'),r'] = \textit{una función divisible por } f(V',r').$$

Habiendo establecido esto, yo digo que obtenemos el grupo relativo a r' al poner a trabajar la misma sustitución de letras a lo largo del grupo relativo a *r*.

En efecto, si por ejemplo tenemos que

$$\varphi_\mu F(V) = \varphi_\upsilon(V),$$

entonces tenemos que (lema IV)

$$\varphi_\mu F(V') = \varphi_\upsilon(V').$$

Por lo tanto, para pasar de la permutación $[F(V)]$ a la permutación $[F(V')]$ es necesario hacer la misma sustitución que hacemos para pasar de la permutación (V) a la permutación (V').

De esta manera queda demostrado el teorema.

PROPOSICIÓN III

Teorema. Si añadimos todas las raíces de una ecuación auxiliar a una ecuación dada, los grupos en cuestión en el teorema II también tendrán esta propiedad, a saber, que las sustituciones son las mismas en cada grupo.

Uno encontrará la demostración.

PROPOSICIÓN IV

Teorema. Si a una ecuación dada añadimos el valor numérico de una cierta función de sus raíces, el grupo de la ecuación será disminuido de tal manera que no tendrá permutaciones excepto aquellas bajo las cuales esta función es invariante.

En efecto, y siguiendo la proposición I, toda función conocida debe ser invariante bajo las permutaciones del grupo de la ecuación.

PROPOSICIÓN V

Problema. ¿En qué caso es soluble una ecuación por radicales simples?

Primero observaré que, para resolver una ecuación, es necesario disminuir su grupo sucesivamente hasta que contenga no más que una sola permutación. Porque cuando una ecuación es resuelta, es conocida toda función de sus raíces incluso cuando no es invariante bajo cualesquiera permutaciones.

Habiendo establecido esto, busquemos qué condición debe ser satisfecha por el grupo de una ecuación para que pueda ser disminuido de esta manera por la añadidura de cantidades radicales.

Sigamos la secuencia de posibles operaciones en esta solución, considerando la extracción de cada raíz de grado primo como una operación distinta.

Añadamos a la ecuación original el primer radical extraído en la solución. Entonces dos situaciones son posibles: o bien, por la añadidura de este radical, disminuirá el grupo de permutaciones de la ecuación, o bien el grupo seguirá siendo el mismo si esta extracción de la raíz es sólo una simple preparación para la resolución de la ecuación.

Siempre debe haber una disminución del grupo después de sólo un cierto número *finito* de extracciones, a menos que la ecuación no sea soluble.

Si, habiendo llegado a este punto, debe haber muchas formas de disminuir al grupo de la ecuación dada por una simple extracción de una raíz, será necesario, para lo que vamos a decir, considerar solamente un radical del menor grado posible entre todos

los radicales simples tales que el conocimiento de cada uno de ellos disminuye al grupo de la ecuación.

Así, sea *p* el número primo que representa este grado mínimo en una situación en la que disminuimos al grupo de la ecuación por una extracción de una raíz de grado *p*.

Siempre podemos suponer, por lo menos con respecto al grupo de la ecuación, que una *p*-ésima raíz de unidad α ha de encontrarse entre las cantidades previamente añadidas a la ecuación. Porque, ya que esta expresión se obtiene por las extracciones de raíces de grado menor que *p*, su ser-conocida no alterará en absoluto al grupo de la ecuación.

Consecuentemente, y después de los teoremas II y III, el grupo de la ecuación debe descomponerse en *p* grupos tendiendo esta doble propiedad entre sí:

(1) que pasamos de uno a otro por una sola sustitución

(2) que todos ellos contienen las mismas sustituciones.

A la inversa, yo digo que si el grupo de la ecuación puede ser partido en *p* grupos que tienen esta doble propiedad, podremos reducir al grupo de la ecuación a uno de los grupos parciales por una simple extracción de la *p*-ésima raíz y por la añadidura de esta *p*-ésima raíz.

En efecto, tomemos una función de las raíces que es invariante bajo todas las sustituciones de uno de los grupos parciales y que varía de acuerdo con cada otra sustitución. (Para esto es suficiente con elegir una función simétrica de los distintos valores tomados por una función que no es invariante bajo ninguna sustitución por cualquier permutación de uno de los grupos parciales.)

Sea θ esta función de las raíces.

Pongamos a trabajar, sobre la función θ, una de las sustituciones del grupo total que no es compartida por el grupo parcial. Sea θ_1 el resultado de esta sustitución. Pongamos a trabajar la misma sustitución sobre la función θ_1 y sea θ_2 el resultado, y así sucesivamente.

Ya que *p* es un número primo, esta serie podrá detenerse sólo en el término θ_{p-1}, después de lo cual tendremos que $\theta_p = \theta, \theta_{p+1} = \theta_1$, y así sucesivamente.

Habiendo dicho esto, es claro que la función

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + ... + \alpha^{p-1}\theta_{p-1})^p$$

será invariante bajo todas las permutaciones del grupo total y, consecuentemente, será realmente conocida.

Si extraemos la *p*-ésima raíz de esta función y la añadimos a la ecuación dada, entonces, por la proposición IV, el grupo de la ecuación no contendrá otras sustituciones sino aquellas del grupo parcial.

Así, para que el grupo de una ecuación pueda ser disminuido por una simple extracción de una raíz, esta misma condición es necesaria y suficiente.

Añadamos a la ecuación original el radical en cuestión; ahora podremos razonar acerca de este nuevo grupo como acerca del anterior, y será necesario que sea partido de la manera indicada arriba, y así sucesivamente, hasta un cierto grupo que no contendrá más que una sola permutación.

Escolio. Es fácil observar esta secuencia en la ya conocida resolución de la ecuación general de cuarto grado. En efecto, estas ecuaciones son resueltas por medio de una ecuación de tercer grado, que en sí misma requiere la extracción de una raíz cuadrada para su resolución. En la serie natural de ideas, es necesario comenzar con esta raíz cuadrada. Pero, al añadir esta raíz cuadrada a la ecuación de cuarto grado dada, el grupo de la ecuación, que contiene veinticuatro permutaciones totales, es partido en dos grupos cada uno de los cuales contiene sólo doce. Designando a las raíces con *a*, *b*, *c*, *d*, uno de estos dos grupos más pequeños es:

abcd, *acdb*, *adbc*,
badc, *cabd*, *dacb*,
cdab, *dbac*, *dcab*,
dcba, *bdca*, *cbda*.

Ahora, este mismo grupo puede ser partido en tres grupos tal como se indicó en los teoremas II y III. Así, por la extracción de un solo radical de tercer grado, simplemente queda el grupo

abcd,
badc,
cdab,
dcba;

este grupo es partido de nuevo en dos grupos

abcd, *cdab*,
badc, *dcba*.

Y así, después de una simple extracción de una raíz cuadrada, quedará

abcd,

badc,

que al final será resuelto por una simple extracción de una raíz cuadrada.

De esta manera obtenemos, o bien la solución de Descartes, o bien la de Euler, porque, aunque después de la resolución de la ecuación auxiliar de tercer grado Euler extrae tres raíces cuadradas, sabemos que dos son suficientes porque la tercera puede deducirse racionalmente.

Ahora aplicaremos esta condición a ecuaciones irreducibles de grado primo.

Aplicación a ecuaciones irreducibles de grado primo.

PROPOSICIÓN VI

Lema. Una ecuación irreducible de grado primo no puede volverse reducible por la añadidura de un radical cuyo índice no es otro que el mismo grado de la ecuación irreducible dada.

Porque si $r, r', r'',...$ son los distintos valores del radical y $Fx = 0$ es la ecuación irreducible de grado primo dada, para Fx es necesario partirse en factores

$$f(x,r)\times f(x,r')\times ...$$

cada uno del mismo grado, lo que no es posible a menos que $f(x,r)$ sea una ecuación de grado primo en *x*.

Así, una ecuación irreducible de grado primo no puede volverse reducible a menos que su grupo se reduzca a una sola permutación.

PROPOSICIÓN VII

Problema. ¿Cuál es el grupo de una ecuación irreducible de grado primo n si es soluble por radicales?

Después de la proposición precedente podemos decir que el grupo más pequeño posible antes del grupo que sólo tiene una sola permutación contendrá *n* permutaciones. Pero un grupo de permutaciones de un número primo *n* de letras no puede ser reducido por *n* permutaciones a menos que cada una de estas permutaciones pueda ser deducida de otra por una sustitución cíclica de orden *n* (véase la memoria del señor Cauchy, *Journal de l'Ecole Polytechnique*, volumen XVII). De esta forma, el penúltimo grupo será

$$
\text{(G)}\quad
\begin{array}{cccccccc}
x_0, & x_1, & x_2, & x_3, & ,\ldots, & x_{n-3}, & x_{n-2}, & x_{n-1}, \\
x_1, & x_2, & x_3, & x_4, & ,\ldots, & x_{n-2}, & x_{n-1}, & x_0, \\
x_2, & x_3, & \ldots & \ldots & ,\ldots, & x_{n-1}, & x_0, & x_1, \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
x_{n-1}, & x_0, & x_1, & \ldots & ,\ldots, & x_{n-4}, & x_{n-3}, & x_{n-2},
\end{array}
$$

$x_0, x_1, x_2, \ldots, x_{n-1}$ siendo las raíces de la ecuación irreducible dada.

Ahora bien, el grupo que inmediatamente precederá a este grupo en el orden de ser partido debe estar compuesto de un cierto número de grupos teniendo todos las mismas sustituciones que este grupo. Pero observo que estas sustituciones pueden expresarse de esta manera: (En general, establezcamos que $x_n = x_{n+1} = x_i, \ldots$. Es claro que cada una de las sustituciones de un grupo (G) pueden obtenerse poniendo x_{k+c} en lugar de x_k, c siendo una constante.)

Consideremos uno de los grupos similares al grupo (G). Siguiendo el teorema II, obtendremos el grupo similar al poner a trabajar la misma sustitución en todos lados en este grupo; por ejemplo, al poner $x_{f(k)}$ en lugar de x_k en todos lados en el grupo (G), f siendo una cierta función.

Como las sustituciones de este nuevo grupo deben ser las mismas que las del grupo (G), debemos tener que

$$f(k+c) = f(k) + C\,,$$

C siendo independiente de k.

Así,

$$f(k+2c) = f(k) + 2C$$

$$\cdots$$

$$f(k+mc) = f(k) + mC.$$

Si $c = 1, k = 0$, encontraremos que

$$f(m) = am + b$$
$$f(k) = ak + b,$$

a y b siendo constantes.

De esta manera el grupo que inmediatamente precede al grupo (G) debe contener sólo sustituciones como

$$x_k, x_{ak+b},$$

y no contendrá, consecuentemente, ninguna sustitución cíclica salvo aquella del grupo (G).

Razonaremos acerca de este grupo tal como lo hacemos con el anterior, y se seguirá que el primer grupo en el orden de ser partido, esto es, el grupo *real* de la ecuación, sólo puede contener sustituciones de la forma

$$x_k, x_{ak+b}.$$

Así, si una ecuación irreducible de grado primo es soluble por radicales, el grupo de esta ecuación sólo puede tener sustituciones de la forma

$$x_k, x_{ak+b},$$

a y b siendo constantes.

A la inversa, si esta condición está en su lugar, yo digo que la ecuación será soluble por radicales. En efecto, consideremos las funciones

$$(x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{x-1} x_{n-1})^n = X_1,$$
$$(x_0 + \alpha x_a + \alpha^2 x_{2a} + \ldots + \alpha^{n-1} x_{(n-1)_a})^n = X_a,$$
$$(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + \ldots + \alpha^{n-1} x_{(n-1)a^2})^n = X_{a^2},$$

α siendo una n-ésima raíz de la unidad y a una raíz primitiva de n.

En este caso es claro que toda función que es invariante bajo las sustituciones cíclicas de las cantidades $X_1, X_a, X_{a^2},\ldots$ será inmediatamente conocida. De esta forma podremos encontrar $X_1, X_a, X_{a^2},\ldots$ por el método del Sr. Gauss para ecuaciones binomiales. Por lo tanto, etcétera.

Así, para que una ecuación irreducible de grado primo sea soluble por radicales, es necesario y suficiente que toda función invariante bajo las sustituciones

$$x_k, x_{ak+b}$$

sea conocida racionalmente.

Así pues, la función

$$(X_1 - X)(X_a - X)(X_{a^2} - X)$$

debe ser conocida sin importar qué sea X.

Es necesario y suficiente, por tanto, que la ecuación que da esta función de raíces admita un valor raciones sin importar qué sea X.

Si la ecuación dada tiene todos coeficientes racionales, la ecuación auxiliar que da esta función también tendrá todos coeficientes racionales, y será suficiente con

reconocer si esta ecuación auxiliar de grado $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-2)$ tiene o no una raíz racional, y ya sabemos cómo hacer eso.

Aquí están los medios necesarios para su uso práctico. Pero presentaremos el teorema, una vez más, bajo otra forma.

PROPOSICIÓN VIII

Teorema. Para que una ecuación irreducible de grado primo sea soluble por radicales, es necesario y suficiente que, cuando cualesquiera dos de sus raíces son conocidas, las demás puedan deducirse racionalmente.

En primer lugar, es necesario porque, ya que la sustitución

$$x_k, x_{ak+b}$$

no permite que cualesquiera dos letras sean puestas en el mismo lugar, es claro, por la proposición IV, que al añadir dos raíces a la ecuación su grupo debe reducirse a sólo una permutación.

En segundo lugar, es suficiente porque, en este caso, cualquier otra sustitución de este grupo no permitirá que dos letras permanezcan en el mismo lugar. Consecuentemente, el grupo contendrá a lo mucho $n(n-1)$ permutaciones. Así, contendrá sólo una sola sustitución cíclica (sin la cual tendría por lo menos n^2 permutaciones). De esta manera, toda sustitución del grupo x_k, x_{fk} debe satisfacer la condición

$$f(k+c) = fk + C\ .$$

Por lo tanto, etcétera.

De esta forma queda demostrado el teorema.

Ejemplo del teorema VII.

Sea $n=5$; entonces el grupo será el siguiente:

abcde

bcdea

cdeab

deabc

eabcd

acebd

cebda

ebdac

bdace

daceb

aedcb

edcab

edcba

dcbae

cbaed

baedc

adbec

dbeca

becad

ecadb

cadbe

———.